Practical Limits of the Secret Key-Capacity for IoT Physical Layer Security

George Margelis*, Xenofon Fafoutis*, Robert J. Piechocki*, George Oikonomou*, Theo Tryfonas*, Paul Thomas†
*Communication Systems and Networks Research Group
MVB, School of Engineering
University of Bristol, UK
†University of Bristol Honorary Research Fellow
george.margelis@bristol.ac.uk

***Abstract*—The confidentiality of communications in the Internet of Things (IoT) is critical, with cryptography being currently the most widely employed method to achieve it. Establishing cryptographically secure communication links between two transceivers requires the pre-agreement on some key, unknown to an external attacker. In recent years there has been growing interest for techniques that generate a shared random key through observation of the channel and its effects on the exchanged messages. The maximum length of that key is characterised by the Mutual Information (MI) between the observations of the two radios. In this work we examine the practical limits of the MI of off-the-shelf transceivers communicating through the IEEE 802.15.4 specification in an indoor office environment, and calculate the secret-key capacity, that is, the maximum length of an extracted secret-key in the presence of an eavesdropper. Furthermore, we study how using groups of observations can affect the MI and both analytically and experimentally prove that grouping observations leads to better results and an increased key-capacity.**

I. Introduction

The vision of an Internet of Things (IoT) is coming closer to realisation with each passing day, where physical objects will have virtual representations, they will be controlled remotely and act as physical access points to Internet services [1]. Thus the physical world will be controllable through the virtual one. However, this introduces new risks since attackers can potentially gain access to systems considered so far as secure. Furthermore the broadcasting nature of wireless sensor networks (WSN), that will form a large part of the IoT, makes communications prone to eavesdropping, increasing the need for confidentiality, which currently is accomplished by cryptographic schemes.

However the nodes that will comprise these WSN are often weak, both in terms of computational capabilities and security measures, as they are very constrained in hardware space, processor power and battery life. Thus security services that reside in the higher levels of the OSI model, such as traditional cryptographic protocols that require key distributions or certificate management [2], might not be sufficiently efficient for IoT devices. Due to this, in recent years there has been a renewed effort into devising security schemes that reside in the physical layer and can supplement novel lightweight cryptographic protocols [3], [4], [5].

A promising direction seems to be using observations of the common channel between two transceivers to agree to a bit sequence that can be then used as a seed for a cryptographic primitive or as an encryption key. Using the theory of reciprocity for antennas and electromagnetic propagation, and assuming that bidirectional transmissions occur inside the coherence time, methods [6], [7] have been proposed for the communicating parties to agree to a key based on the channel impulse response. The maximum size of a binary sequence that can be shared this way is characterised by the MI between the observations of the two radios.

In the past, theoretical work has been done in calculating the upper bound of the MI for a variety of channels [8], [9], [10]. However, there is still no work that examines the achievable MI with off-the-shelf components in real-life implementations. Past experimental works in the field have attempted to measure the entropy of the Received Signal Strength Indicator (RSSI) observations as an indication of the length of the extracted shared bit sequence, however they need to rely on Forward Error Correction (FEC) to correct errors that result from inconsistencies between the two extracted sequences. Measuring the MI, takes this one step ahead, by quantifying the circumstances when FEC is less or more necessary.

In this work we initially measure the MI of two IEEE 802.15.4 transceivers that use the Texas Instrument's CC2650 System-on-Chip (SoC) [11]. Due to the nature of the transceivers the only observation of the channel that can be done without additional hardware is a measurement of the RSSI of every received packet. This paper makes the following contributions:

- We calculate the MI of the RSSI measurements of two communicating parties with and without knowledge of the RSSI values of the eavesdropped packets. This allows us to quantify both the maximum key length that can be agreed upon, as well as the maximum key length that can be agreed in secrecy from an eavesdropper.
- We study the effects of using groups of different size of RSSI values instead of point-values as observations, and its effects on the MI between the two communicating parties and derive an expression for the MI of groups of observations under the assumption of stationarity.

The rest of the paper is organised as follows: Section II covers prior work in the domain. Section III defines the threat model and the characteristics of the eavesdropper, while Section IV provides a short introduction to MI and key-rates. Section V describes our methodology and experimental set-up, and presents our results, followed by Section VI where we present our work on vectoring and its effects on MI. Finally Section VII includes our conclusions.

II. Prior work

The idea of generating a shared random key at two terminals, by exploiting some common randomness of the communicating medium has been examined in the past. Ahlswede and Csiszár in [9] and [10] published some of the seminal work on the field where they explored the generation of common randomness by two terminals without giving information about it to a third party. They also defined the concept of key-capacity, that is the maximum rate of the generation of a secret key by a pair of terminals observing correlated sources, and proved that in the case of a Discreet Memoryless Multiple Source Model (DMMS) the key-capacity is equal to the MI.

Their work was extended in [8] by quantifying the theoretical upper bounds of the length of the common randomness in bits for ultrawideband channels. The authors calculate the MI and use it to characterise the maximum key size that can be shared through observations of the channel pulse response.

The aforementioned works focus on finding the upper bounds of the MI. However these bounds are only theoretically possible and practically unattainable without using specialised equipment. The maximum size as well as generation of shared secret keys from the observation and processing of radio channel parameters have also been examined in [7], [12], [13], [14]. However the aforementioned works examine the subject either purely from a theoretical informational-theoretic perspective, or by performing the observations with specialised hardware. In contrast, our work is the first to use experimental results with off-the-shelf components designed for IoT applications, to measure MI between two terminals.

III. Threat Model

Calculating the MI between the observations of a random variable by two communicating parties is important to quantify the size of the bit sequence that they can agree upon, however from a security perspective we are interested more in the size of the key that can be agreed in secret from an eavesdropper.

Before we continue then, we need to define the eavesdropper's abilities. We assume that the eavesdropper, Eve, can listen to all communications between the legitimate communicating parties, Alice and Bob. We also assume that the eavesdropper can record the RSSI values of the overheard messages. We make no assumptions on the location of Eve in relation to Alice or Bob, apart from the fact that Eve is at least further than the coherence distance from both of them [15]. Furthermore we assume that Eve is completely passive, that is, she does not attempt to jam the medium, inject traffic or in general transmit at any time. We make no assumption on the hardware capabilities of Eve. For the rest of this paper the terms Alice, Bob and Eve are used interchangeably with A, B and E respectively.

IV. Mutual Information and Key-Capacity

A. Key-Capacity

The mutual information $I(X;Y)$ is the reduction in the uncertainty of X due to the knowledge of Y (and the inverse) and can be expressed as:

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) \ , \quad (1)$$

where

$$H(X) = -\sum_{x\in X} p(x) log_2 p(x) \ , \quad (2)$$

$$H(Y) = -\sum_{y\in Y} p(y) log_2 p(y) \ , \quad (3)$$

and

$$H(X|Y) = -\sum_{y\in Y}\sum_{x\in X} p(x,y) log_2 p(x|y) \ . \quad (4)$$

$H(Y|X)$ can be expressed similarly. We use the observed frequencies of x and y for the calculation of $p(x)$ and $p(y)$.

In other words, $I(X;Y)$ quantifies the "amount of information" (in bits) obtained about one random variable, through the other random variable, but also $I(X;Y)$ is the Key-Capacity, that is the maximum achievable key-rate, as defined in [9]. In our case the random variables are measurements of the RSSI of every packet exchanged. Thus, X is the sequence of RSSI values measured by Alice, and Y the sequence of RSSI values measured by Bob. Unfortunately, we are limited in the time resolution of the RSSI measurements, as current off-the-shelf wireless transceivers report RSSI per frame and not per symbol.

If X and Y were independent and uncorrelated, we would expect $I(X;Y)$ to be zero, however that is not the case due to the reciprocity of the channel. Furthermore from (1) we can see that the attainable MI is upper-bounded by the entropy of the two sources. Hence, scenarios where $H(X)$, $H(Y)$ are higher can potentially lead to higher key-capacities.

B. Secret Key-Capacity

If Alice and Bob wish to agree to a key that is kept secret from an eavesdropper, Eve, then the upper bound might not be equal to $I(X;Y)$. Assume that Eve observes the transmitted packets and logs their RSSI values, $z_x \in Z_x$ and $z_y \in Z_y$ respectively for X and Y. Then the secret key-capacity is upper bounded [8] by

$$\begin{aligned} K(X;Y||Z) = \min[&I(X;Y), I(X;Y|Z_x), \\ &I(X;Y|Z_y), I(X;Y|Z_x Z_y)] \ . \end{aligned} \quad (5)$$

It is important to remember that $I(X;Y|Z)$ can be smaller or bigger than $I(X;Y)$. We should also keep in mind that due to packet loss, it is possible for Eve to fail to capture some of the exchanged packets. Aiming to study the worst case scenario, in this work, we assume that Eve is able to log all of the

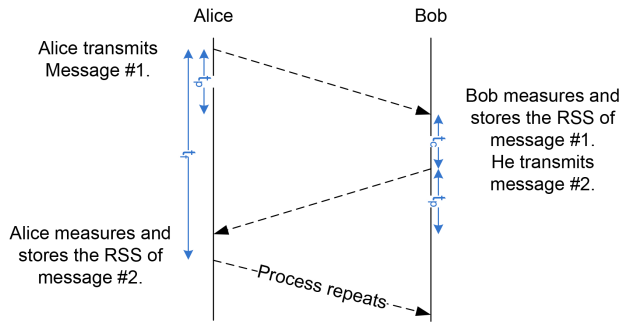

Fig. 1. The methodology of RSSI logging.

packets. Practically, we implement this by considering only the packets that were successfully received by the eavesdropper in the calculations of the MI.

V. Implementation and Experimental Results

We implemented our system on three SmartRF06 evaluation boards [16] using the CC2650 radio [11]. Two of the boards act as Alice and Bob, while the third acts as Eve. In Figure 2, we detail the spatial arrangement of Alice, Bob and Eve in each scenario.

Commercial wireless transceivers are currently half-duplex, thus the logged RSSI values correspond to messages that have a small time delay of each other. The process of message exchange can be seen in Figure 1, where t_p is the transmission delay, t_c the time needed for Bob to measure the RSSI value of the message and respond with another message, and t_f the time between two successive beacon messages sent by Alice. To ensure the reciprocity of radio wave propagation we have to keep t_c as small as possible. For the purposes of this work $t_p = 2.4$ ms while $t_c = 7.8$ ms and $t_f = 1$ s.

A. Scenario 1: Anechoic Chamber

As an initial step we examine the results of our experiment in a completely isolated and static environment to verify the basic assumption of our work, *i.e.* the main source of randomness in the observations is the channel. To ensure that there is no interference we use the anechoic chamber of the University of Bristol. The layout of the experiment can be seen in Figure 2 (right). In such environment, we expected minimal to no variations of RSSI. Our measurements verified our expectations, as can be seen in the first scatter plot in Figure 4 where we can see that both sequences of observations alternated between only two values.

Specifically, in Figure 3 we observe that the RSSI of the packets that were received by Alice have zero variance, thus the entropy is zero. It follows then, that the MI is also zero. Yet, the RSSI of the packets received by Bob deviates between two values. We attribute this to the effects of thermal noise (which are independent sources of noise present in both Alice and Bob). Indeed, it is possible that, contrary to Bob, these variations are not sufficient to cross the quantisation threshold in Alice's measurements.

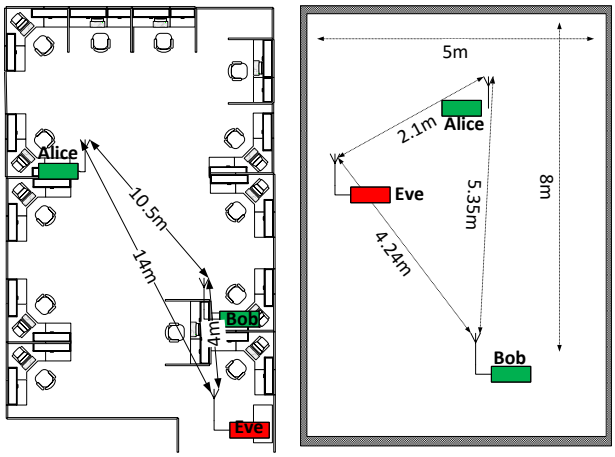

Fig. 2. Left: Layout of experiment in office space. Right: Layout of experiment in the anechoic chamber.

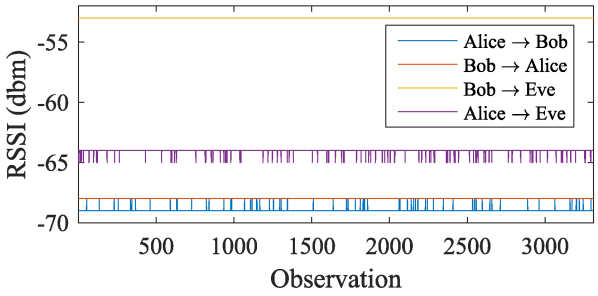

Fig. 3. RSSI of packets exchanged in the anechoic chamber.

Eve is passively eavesdropping all the transmitted messages. Being herself immobile and passive, Eve does not affect the channel in any way. Thus, we expect little to no variations in the logged values. Again, the results support our expectations, as it can been seen in Figure 3. The difference in the absolute values is the result of different distances between Alice and Bob, which lead to different path loss.

We can observe that the packets received from Bob have a constant RSSI of -53 dBm, whilst the RSSI of the packets received from Alice alternate between two values, -65 dBm and -64 dBm. The fact that this variation bears no correlation to the aforementioned (correlation coefficient is 0.0141) indicates that it is indeed the result of random thermal noise. This also implies that there is potentially randomness in our observations that is not a result of the channel, however is uncorrelated and not shared. Hence, this randomness does not increase the MI, which in this case is zero.

B. Scenario 2: Office Space

We proceed now on a more realistic scenario: an open office space whose layout can be seen in Figure 2 (left). This scenario represents a very likely application, especially as IoT devices find themselves in residential and commercial locations. We examine two different scenarios:

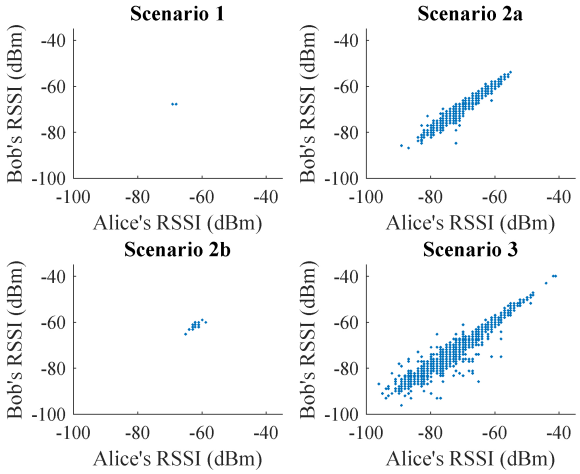

Fig. 4. Scatterplots of the unique pairs of RSSI values exchanged between Alice and Bob in the different scenarios. Scenario 1 (top left) corresponds to the anechoic chamber. Scenario 2a (top right) corresponds to the experiments in the office space during working hours. Scenario 2b (bottom left) corresponds to the experiments in the office space during non-working hours. Scenario 3 (bottom right) corresponds to the experiment with mobile terminals.

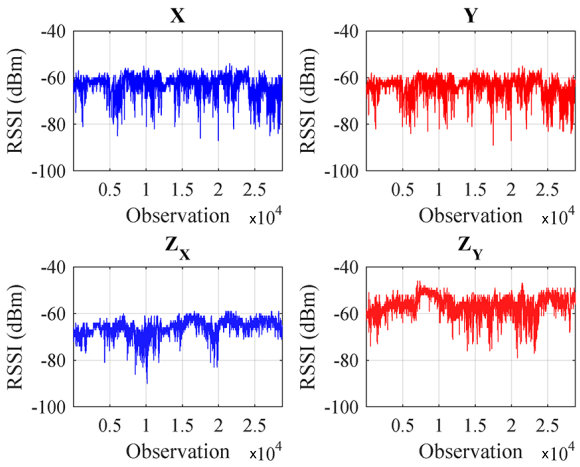

Fig. 5. RSSI of packets captured in the office space during working hours. Top left: RSSI logged by Alice. Top right: RSSI logged by Bob. Bottom left: RSSI logged by Eve from eavesdropped packets directed to Alice. Bottom right: RSSI logged by Eve from eavesdropped packets directed to Bob.

- During working hours, when the office is more busy, and people are moving in the office and in outside spaces.
- After working hours, when there is minimum-to-no activity both in the office and in the surroundings of it.

For each case we examine situations where either there is or there is no Line-of-Sight (LoS) between Alice, Bob and Eve.

1) Working hours: For the purposes of this work we define working hours between 09:00 and 17:00. As we would expect this is the most dynamic of the two cases, as is illustrated in Figures 5 and 4 where we can see the resulting RSSI values and their correlation correspondingly. In this case, people are working in their offices with frequent movement while Alice, Bob and Eve all have LoS. The MI is 2.5009 bits while the minimum entropy between Alice's and Bob's observations is Alice's, being 3.6389 bits. The secret-key capacity is 2.4729 bits.

2) Non-Working hours: We define as night hours the time from 00:00 to 06:00. This part of the experiment bears similarities to the experiment in the anechoic chamber, since although there are a number of multipaths, there are very few variations in the environment, leading to a relatively static channel. This is illustrated in Figure 4 where we can see that we have a reduced number of unique measured values. The MI is 0.1964 bits with the minimum entropy between the two sets of observations being 0.7805 bits, from Bob's observations while the secret-key capacity is 0.1665 bits.

C. Scenario 3: Mobile terminals

In the last scenario we examine the communication between a stationary base-station and a mobile terminal. This scenario was run in two different circumstances, with the results being fairly similar. As Alice is moving around and out of the office space, LoS is lost and re-established, the pathways change

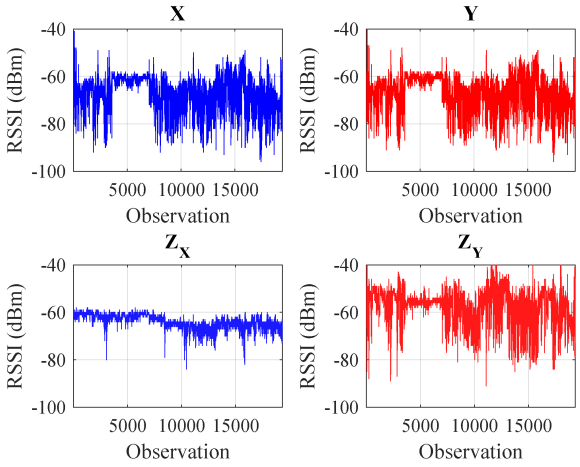

Fig. 6. RSSI of packets exchanged between Alice and Bob when Alice is mobile. Top left: RSSI logged by Alice. Top right: RSSI logged by Bob. Bottom left: RSSI logged by Eve from eavesdropped packets directed to Alice. Bottom right: RSSI logged by Eve from eavesdropped packets directed to Bob.

and thus we would expect to see great variation in the logged RSSI values. Indeed, the results back our expectations as can be seen in the last scatterplot of Figure 4 and in Figure 6.

The MI in the first run is 3.1289 bits, while the entropy of Alice's observations is 4.5416 bits. The secret-key capacity is 2.9187 bits. This scenario results in the highest amount of entropy and mutual information, a result of the much more dynamic nature of the channel due to the movement of Alice.

D. Summary

The results of all our experiments are summarised in Table I. Overall, it can be observed that dynamic scenarios, such as an office during working hours and a mobile terminal,

TABLE I

SUMMARY OF OUR RESULTS FOR ALL SCENARIOS. X IS THE SEQUENCE OF OBSERVATIONS BY ALICE, Y THE SEQUENCE OF OBSERVATIONS BY BOB AND Z_x, Z_y THE SEQUENCE OF OBSERVATIONS BY EVE OF PACKETS THAT FORM X AND Y RESPECTIVELY. THE PRACTICAL SECRET KEY-CAPACITY FOR EACH SCENARIO, AS DEFINED IN (5), IS MARKED IN RED.

Scenario	$\min(H(X), H(Y))$	I(X;Y)	I(X;$Y\|Z_x$)	I(X;$Y\|Z_y$)	I(X;$Y\|Z_x, Z_y$)
Office: Working hours					
A,B and E have LoS	3.6389	2.5009	2.4909	2.5030	**2.4739**
A,B have LoS, E without LoS	3.6348	2.5662	2.5462	2.4700	**2.4247**
A,B and E without LoS	3.8684	2.8507	2.6780	2.8214	**2.5926**
Office: Non-Working hours					
A,B and E have LoS	0.7805	0.1964	0.1761	0.1817	**0.1665**
A,B have LoS, E without LoS	1.3118	0.4615	0.4624	**0.4594**	0.4613
A,B and E without LoS	1.0038	0.2668	0.1603	0.2661	**0.1595**
Mobile Scenario 1	4.5416	3.1289	3.0799	3.0635	**2.9187**
Mobile Scenario 2	4.8330	3.3073	3.3574	3.3963	**3.0517**

practically yield a relatively high secret-key capacity of up 3.0517 bits. We next proceed with considering groups of sequential observations as a means to further increase the secret-key capacity.

VI. GROUPING OBSERVATIONS

In the previous sections we assumed that the observations that form X and Y are point-values of the RSSI. However, we can instead choose to use groups of RSSI values for each observation. Thus instead of $p(x)$ resulting from a distribution of measurements, it is the result of a distribution of vectors, increasing the dimensionality of our observations.

Assume, for example, that we aim to use two subsequent RSSI values as an observation x_i. Then $x_i = [RSSI_i, RSSI_{i+1}]$ where $i \in [1, 3, 5..N-1]$ and N the number of RSSI observations. In this case the set of X is comprised by 807 unique elements in the scenario of working hours in an office (Section V-B1), while without vectoring the set is comprised by only 62 unique elements. However the number of our samples has now been halved. X is no longer a vector $1 \times N$ but a matrix $2 \times (N/2)$. The MI in this case is 5.7875 bits with the entropy of X now reaching 8.0402 bits.

The effects of using groups of different sizes to the MI are presented in Figure 7, while the ratio of MI of groups of observations over the MI of point values is presented in Figure 8. For example, for the mobile scenario (Section V-C), the MI of groups of observations can get as high as 10.68 bits while the MI of point-values was only 3.12 bits. We prove analytically in the appendix the benefit of using groups of observations instead of point values.

VII. CONCLUSIONS

In recent years there has been a renewed focus in physical layer security schemes that can supplement lightweight cryptographic protocols for IoT applications. Extracting a shared bit sequence through observations of the wireless medium is a promising direction in that regard, and the upper limit of the size of that bit sequence, known as key-capacity, is characterised by the MI between the observations of the two communicating parties.

In this work, we have examined the MI between two off-the-shelf wireless transceivers that employ IEEE 802.15.4 radios

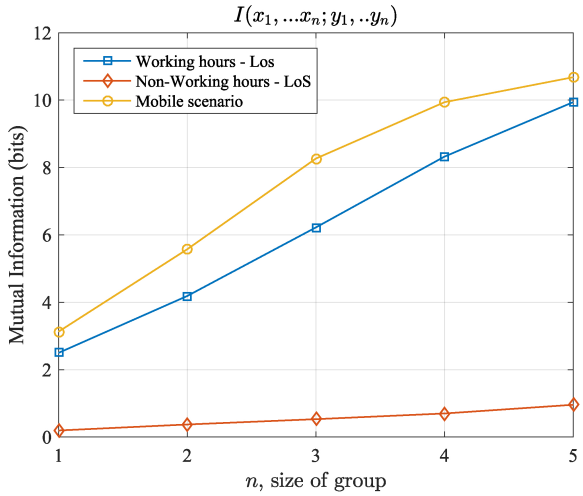

Fig. 7. Effects of using sequences of different sizes of RSSI values as x_i.

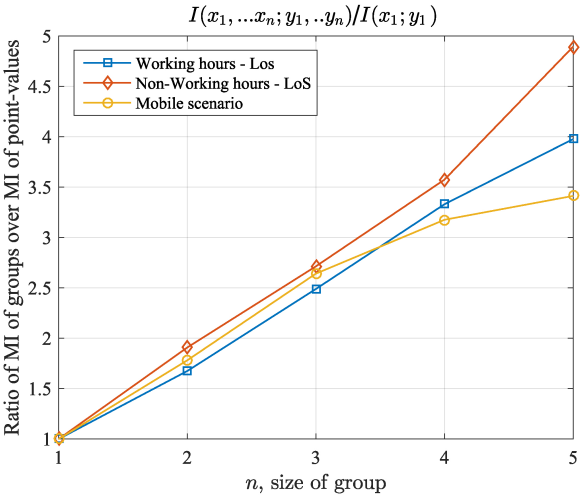

Fig. 8. Ratio of MI of groups over MI of point-values as x_i increases.

to communicate, in real-life experiments and in a variety of situations. Furthermore we explore the effects of vectoring observations to the key-capacity. We analytically prove that this leads to better results for stationary sequences, and nu-

merically show that our stationary model produces sequences that closely follow the entropy and mutual information of our observed sequences. Vectoring the observations logged from a mobile client was shown to lead to mutual information of up to 10.68 bits, while using scalars for the same application resulted in mutual information of only 3.12 bits.

To the best of our knowledge this is the first work that employs off-the-shelf components to measure the MI, and that explores the effects of grouping observations with experimental results, thus making our results immediately applicable to on-the-field implementations.

APPENDIX

We proceed to prove that the MI of groups of observations is always greater or equal to MI of scalars under the assumption of stationarity. We know that

$$I(x_n; y_n) = H(x_n) + H(y_n) - H(x_n, y_n) \tag{6}$$

thus

$$\begin{aligned} I(x_n, x_{n+1}; y_n, y_{n+1}) =& H(x_n, x_{n+1}) + H(y_n, y_{n+1}) \\ & - H(x_n, x_{n+1}, y_n, y_{n+1}) \end{aligned} \tag{7}$$

However,

$$\begin{aligned} H(x_n, x_{n+1}, y_n, y_{n+1}) =& H(x_n, y_n) + H(x_{n+1}, y_{n+1}) \\ & - I(x_n, y_n; x_{n+1}, y_{n+1}) \end{aligned} \tag{8}$$

Substituting (8) in (7):

$$\begin{aligned} I(x_n, x_{n+1}; y_n, y_{n+1}) =& H(x_n) + H(x_{n+1}|x_n) \\ & + H(y_n) + H(y_{n+1}|y_n) \\ & - H(x_n, y_n) - H(x_{n+1}, y_{n+1}) \\ & + I(x_n, y_n; x_{n+1}, y_{n+1}) \end{aligned}$$

and because of (6):

$$\begin{aligned} I(x_n, x_{n+1}; y_n, y_{n+1}) =& I(x_n; y_n) + I(x_n, y_n; x_{n+1}, y_{n+1}) \\ & + H(x_{n+1}|x_n) + H(y_{n+1}|y_n) \\ & - H(x_{n+1}, y_{n+1}) \end{aligned} \tag{9}$$

However under the assumption of stationarity

$$Px_{n+1}y_{n+1} = Px_n y_n \Rightarrow H(x_{n+1}, y_{n+1}) = H(x_n, y_n)$$

and

$$I(x_n, y_n; x_{n+1}, y_{n+1}) = H(x_{n+1}, y_{n+1}) \tag{10}$$

and substituting (10) in (9) we get

$$\begin{aligned} I(x_n, x_{n+1}; y_n, y_{n+1}) =& I(x_n; y_n) + H(x_{n+1}, y_{n+1}) \\ & + H(x_{n+1}|x_n) + H(y_{n+1}|y_n) \\ & - H(x_{n+1}, y_{n+1}) \Rightarrow \end{aligned}$$

$$\begin{aligned} I(x_n, x_{n+1}; y_n, y_{n+1}) =& I(x_n; y_n) + \\ & H(x_{n+1}|x_n) + H(y_{n+1}|y_n) \end{aligned} \tag{11}$$

where $H(x_{n+1}|x_n) \geq 0$ and $H(y_{n+1}|y_n) \geq 0$. $\square$

The exact calculation of the entropy rates $H(x_{n+1}|x_n)$ and $H(y_{n+1}|y_n)$ requires the calculation of the Kolmogorov-Sinai entropies of the time series comprised by the RSSI measurements and is out of scope for this paper.

ACKNOWLEDGMENT

This work was supported by the University of Bristol and the Engineering and Physical Sciences Research Council (EPSRC) through grant EP/I028153/1 and the SPHERE IRC, grant EP/K031910/1.

REFERENCES

[1] F. Mattern and C. Floerkemeier, "From the internet of computers to the internet of things," in *From active data management to event-based systems and more*. Springer, 2010, pp. 242–259.

[2] W. Diffie and M. E. Hellman, "New directions in cryptography," *Information Theory, IEEE Transactions on*, vol. 22, no. 6, pp. 644–654, 1976.

[3] A. F. Skarmeta, J. L. Hernandez-Ramos, and M. Moreno, "A decentralized approach for security and privacy challenges in the internet of things," in *Internet of Things (WF-IoT), 2014 IEEE World Forum on*. IEEE, 2014, pp. 67–72.

[4] M. Abomhara and G. M. Koien, "Security and privacy in the internet of things: Current status and open issues," in *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on*. IEEE, 2014, pp. 1–8.

[5] C. Ye and P. Narayan, "Secret key and private key constructions for simple multiterminal source models," *Information Theory, IEEE Transactions on*, vol. 58, no. 2, pp. 639–651, 2012.

[6] J. Muramatsu, K. Yoshimura, P. Davis, A. Uchida, and T. Harayama, "Secret-key distribution based on bounded observability," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1762–1780, 2015.

[7] A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, "Cryptographic key agreement for mobile radio," *Digital Signal Processing*, vol. 6, no. 4, pp. 207–212, 1996.

[8] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *Information Forensics and Security, IEEE Transactions on*, vol. 2, no. 3, pp. 364–375, 2007.

[9] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. part i: secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, 1993.

[10] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. ii. cr capacity," *Information Theory, IEEE Transactions on*, vol. 44, no. 1, pp. 225–240, 1998.

[11] Texas Instruments, "CC2650 SimpleLink Multistandard Wireless MCU," www.ti.com/lit/ds/symlink/cc2650.pdf, 2015.

[12] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM international conference on Mobile computing and networking*. ACM, 2008, pp. 128–139.

[13] M. G. Madiseh, M. L. McGuire, S. W. Neville, and A. A. B. Shirazi, "Secret key extraction in ultra wideband channels for unsynchronized radios," in *Communication Networks and Services Research Conference, 2008. CNSR 2008. 6th Annual*. IEEE, 2008, pp. 88–95.

[14] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *Information Theory, IEEE Transactions on*, vol. 45, no. 2, pp. 499–514, 1999.

[15] G. D. Durgin and T. S. Rappaport, "Theory of multipath shape factors for small-scale fading wireless channels," *Antennas and Propagation, IEEE Transactions on*, vol. 48, no. 5, pp. 682–693, 2000.

[16] Texas Instruments, "SmartRF06 Evaluation Board User's Guide," www.ti.com/lit/ug/swru321a/swru321a.pdf, 2013.